REMARKS/ARGUMENTS

Prior to entry of this amendment, claims 1, 2, 4-19 and 21-23 were pending in this application. Claims 1, 8, 14, and 23 are amended herein. No claims are canceled or added herein. Therefore, claims 1, 2, 4-19 and 21-23 remain pending in this application. Applicants respectfully request entry of these amendments and reconsideration of this application for at least the reasons presented below.

Generally speaking, the claims have been amended to more clearly define the signing of the first information and the second information or the information object and the authorization information, as well as authenticating such information. More specifically, claim 1 has been amended to include "generating a signatory group comprising at least a portion of a first information and at least a portion of a second information" and indicate that the signature is generated over this signatory group. Similarly, claim 14 has been amended to indicate that "a signatory group is generated comprising at least a portion of the information object and at least a portion of the authorization information" and to indicate that "a signature is generated over the signatory group." Applicants respectfully submit that the references previously cited do not teach or suggest, alone or in combination, generating a signatory group comprising at least a portion of a first information and at least a portion of a second information (or a portion of the information object and a portion of the authorization information) and generating a signature over the signatory group.

Claim 8 has been amended to include "generating a signatory group comprising at least a portion of the first information and at least a portion of the second information" and "calculating a signature from the signatory group" as well as indicating that authenticating the signature over the first and second information is based on the received signature matching the calculated signature. Applicants respectfully submit that the references previously cited do not teach or suggest, alone or in combination, generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature. Each of the previous rejections will now be discussed in light of these amendments.

35 U.S.C. §102 Rejection, Gennaro et al.

The Office Action rejected claims 1 and 8 under 35 U.S.C. §102(b) as being anticipated by the cited portions of Non-Patent Literature document "How to Sign Digital Streams" of Gennaro et al. (hereinafter "Gennaro"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1 and 8 submitted by the Applicant and Gennaro.

As previously stated, Gennaro describes: 1) splitting a stream into blocks; 2) hashing each block and storing the hash value in a table; 3) signing the table; and 4) sending the signed table followed by the stream. However, Gennaro does not disclose generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group as recited in claim 1. Similarly, Gennaro does not disclose generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature as recited in claim 8. For at least these reasons, the Applicant requests that the rejection be withdrawn.

35 U.S.C. §102 Rejection, Wong et al.

The Office Action has rejected claims 1 and 8 under 35 U.S.C. §102(e) as being anticipated by the cited portions of Non-Patent Literature document "Digital Signatures for Flows and Multicasts" of Wong et al. (hereinafter "Wong"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1 and 8 submitted by the Applicant and Wong.

In Wong, packets are successively hashed and the resulting single message digest is signed. However, Wong does not disclose generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group as recited in claim 1. Similarly, Wong does not disclose generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature as recited in claim 8. For at least these reasons, the Applicant requests that the rejection be withdrawn..

<u>35 U.S.C. §102 Rejection, Wasilewski'474</u>

The Office Action has rejected claims 1-2, 4-6, 8-9, 11-13 and 21 under 35 U.S.C. §102(e) as being anticipated by the cited portions of U.S. Patent No. 5,870,474 of Wasilewski et al. (hereinafter "Wasilewski '474"). The Applicant respectfully submits the following arguments pointing out significant differences between claims 1-2, 4-6, 8-9, 11-13 and 21 submitted by the Applicant and Wasilewski '474.

As previously stated, Wasilewski describes a series of successive encryptions in which a first key is used to encrypt a packet, a second key is used to encrypt the first key, and the customer's public key is used to encrypt the second key. Of these keys, Wasilewsi applies a digital signature only to the second key. The encryption of the first key with the multi-session key (MSK) and the encryption of the second key with the user's public key control access to the content but do not affect a signature, only the second key is signed. However, Wasilewski does not disclose generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group as recited in claim 1. Similarly, Wasilewski does not disclose generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature as recited in claim 8. For at least these reasons, the Applicant requests that the rejection be withdrawn and claims 1-2, 4-6, 8-9, 11-13 and 21 be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al.

The Office Action has rejected claims 7, 10, 14-15 and 19 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of U.S. Patent No. 5,247,364 of Banker et al. (hereinafter "Banker"). The Applicant respectfully submits that the Office Action does not establish a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

In order to establish a *prima facie* case of obviousness, the Office Action must establish: 1) some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the references or combine their teachings; 2) a reasonable expectation of success of such a modification or combination; and 3) a teaching or suggestion in the cited prior art of each claimed limitation. See MPEP §706.02(j). As will be discussed in detail below, the references cited by the Office Action do not teach or suggest each claimed limitation.

As discussed above, independent claim 1, upon which claim 7 depends and claim 8, upon which claim 10 depends are distinguishable from Wasilewski. Specifically, Wasilewski does not teach or suggest generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group as recited in claim 1. Similarly, Wasilewski does not teach or suggest generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature as recited in claim 8. Additionally, Wasilewski does not teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group as recited in claim 14.

Banker is directed to "a method and apparatus for tuning channels in a subscription television system having in-band data transmissions." (Col. 1, lines 10-12) Under Banker, an "addressable transmitter transmits data to out-of-band subscriber terminals via a dedicated FM data channel." (Col. 2, lines 55-57) "Scramblers are coupled to headend controller and may be used to selectively scramble television signals for improved security in a subscription television system that is equipped with appropriate descramblers." (Col. 3, lines 47-51) However, Banker does not teach or suggest generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group as recited in claim 1. Similarly, Banker does not teach or suggest generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature as recited in claim 8. Additionally, Banker does not teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group as recited in claim 14.

The combination of Wasilewski '474 and Banker is no more relevant to the pending claims than either reference alone. Neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group as recited in claim 1. Similarly, the combination does not teach or suggest generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature as recited in claim 8. Additionally, the combination does not teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group as recited in claim 14. For at least these reasons, claims 7, 10, 14-15 and 19 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al. further in view of Shear et al.

The Office Action has rejected claims 16 and 17 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Banker and further in view of the cited portions of U.S. Patent No. 6,157,721 of Shear et al. (hereinafter "Shear"). The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 14 upon which claims 16 and 17 depend is distinguishable from Wasilewski '474 and Banker since neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group as recited in claim 14.

Shear is directed to "computer security techniques based at least in part on cryptography, that protect a computer processing environment against potentially harmful computer executables, programs and/or data; and to techniques for certifying load modules such as executable computer programs or fragments thereof as being authorized for use by a protected or secure processing environment." (Col. 1, lines 22-28) Under Shear, "a verifying authority can digitally sign a load module or other executable with several different digital signatures and/or signature schemes." (Col. 7, lines 9-11) That is, "a protected processing environment or other secure execution space may require a load module or other executable to present multiple digital signatures before accepting it." (Col. 7, lines 11-14) In other words, the module may be signed multiple times. However, Shear does not teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group.

The combination of Wasilewski '474, Banker, and Shear is no more relevant to the pending claims than any of the references alone. None of the references, alone or in combination, teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group. For at least these reasons, claims 16 and 17 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski '474 in view of Banker et al. further in view of Wasilewski '866

The Office Action has rejected claim 18 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Banker and further in view of the cited portions of U.S. Patent No. 5,420,866 of Wasilewski (hereinafter "Wasilewski '866). The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 14 upon which claim 18 depends is distinguishable from Wasilewski '474 and Banker since neither Wasilewski '474 nor Banker, alone or in combination, teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group.

Wasilewski '866 "is directed to methods for providing conditional access information to decoders in a packet-based multiplexed communications system." (Col. 5, lines 31-33) Wasilewski teaches "methods for providing a plurality of different sets of conditional access information to a remote location and for facilitating access to a selected one of those sets of conditional access information by a decoder at the remote location." (Col. 5, lines 38-43) However, Wasilewski '866 does not teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group.

The combination of Wasilewski '474, Banker, and Wasilewski '866 is no more relevant to the pending claims than any of the references alone. None of the references, alone or in combination, teach or suggest generating a signatory group comprising at least a portion of an information object and at least a portion of an authorization information and generating a signature over the signatory group. For at least these reasons, claim 18 should be allowed.

35 U.S.C. §103 Rejection, Wasilewski et al. in view of Shear et al.

The Office Action has rejected claims 22 and 23 under 35 U.S.C. §103(a) as being unpatentable over the cited portions of Wasilewski '474 in view of the cited portions of Shear. The Applicant respectfully submits that the Office Action has not established a *prima facie* case of obviousness in rejecting these claims. Therefore, the Applicant requests reconsideration and withdrawal of the rejection.

As discussed above, independent claim 1 upon which claim 23 depends and independent claim 8, upon which claim 22 depends are distinguishable from Wasilewski '474 and Shear since neither Wasilewski '474 nor Shear, alone or in combination, teach or suggest generating a signatory group comprising at least a portion of a first information and at least a portion of a second information and generating a signature over the signatory group as recited in claim 1. Similarly, the combination does not teach or suggest generating a signatory group comprising at least a portion of the first information and at least a portion of the second information, calculating a signature from the signatory group, and authenticating the signature over the first and second information based on the received signature matching the calculated signature as recited in claim 8. For at least these reasons, claims 22 and 23 should be allowed.

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance and an action to that end is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

William J. Daley
Reg. No. 52,471

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000 (Denver office)
Fax: 303-571-4321 (Denver office)

WJD:sbm